ANNEX L

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)

On February 28, 2003, President Bush issued Homeland Security Presidential Directive–5 (HSPD-5), which directed the Secretary of Homeland Security to develop, submit for review, and administer a National Incident Management System (NIMS). This system will provide a consistent nationwide approach for Federal, State, tribal, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. This document establishes the NIMS and provides mechanisms for its further development and for the continuing maintenance of standards, guidelines, and protocols.

Building upon the existing National Interagency Incident Management System (NIIMS), this document integrates best practices that have proven themselves over the years into a comprehensive framework for use by all incident management organizations nation-wide. It also sets in motion the process needed to leverage new technologies and new approaches to continue to refine the NIMS in the future.

NIMS is based on an appropriate mix of both flexibility and standardization.

Flexibility. NIMS provides a consistent and flexible national framework within which all levels of government and private entities can work together to manage domestic incidents, regardless of their cause, size, location, or complexity.

Standardization. NIMS is a set of standardized organizational structures and procedures to improve interoperability among jurisdictions and disciplines. The structures include:

- Incident Command System
- Unified command
- Multi-agency Coordination Systems

The common procedures include:

- Training
- Management of resources
- Qualifications and certification
- Collection, tracking, and reporting of incident and resource information
- Continuous system improvement

The NIMS incorporates existing best practices into a nation-wide, standardized domestic incident management system applicable to all hazards and all levels of government. Six major components provide a systems approach to domestic incident management.

1. NIMS Components.

The following is a synopsis of each NIMS component. A detailed discussion of each component is included in subsequent sections of this document.

a. Command and Management. NIMS standardizes domestic incident management for all risks and all hazards and across all levels of government. NIMS-standard incident command structures are based on two key constructs:

- The Incident Command System (ICS), which defines the operating characteristics, interactive management components, organization, and operations of incident managers and responders engaged at the scene;
- Multi-agency coordination systems, which define the operating characteristics, interactive management components, organizations, and operations of supporting agencies engaged at the local, tribal, State, regional, and Federal levels through mutual-aid agreements and other assistance arrangements.

b. Preparedness. Incident management must begin before an incident takes place. Preparedness requires planning, training, qualifications and certification, and publication management. A synopsis of each of these activities follows:

- Planning: Plans describe how personnel, equipment, and other resources will be used in response to an incident. Plans provide mechanisms for setting priorities, integrating multiple entities and functions, and ensuring that communications and other systems are available to support domestic incident management activities.
- Training: Training includes standard courses on incident command and management, organizational structure, and operational procedures;

discipline-specific and agency-specific courses; as well as providing training required for supporting technologies.

- promulgate, and measure performance against national standards to certify that personnel are qualified to perform NIMS-related functions.
- Publications Management: Publications management refers to developing publication materials, administering publications—including establishing naming and numbering conventions, managing the publication and promulgation of documents, exercising control over sensitive documents, and revising publications when necessary.

c. Resource Management. NIMS defines standardized mechanisms to describe, inventory, track, and dispatch resources before, during, and after an incident.

d. Communications and Information. NIMS establishes a standardized framework for communications, information management (collection, analysis, and dissemination), and information-sharing support to all levels of incident management. These are briefly described as follows:

(1) Incident Management Communications. A system to ensure effective communications support for incident management efforts at all levels.

(2) Information Management. Information management helps ensure that information, including communications and data, flows efficiently between all levels responsible for managing or directing domestic incidents. Effective information management enhances preparedness and response for a domestic incident by providing, promoting, and facilitating information and automation initiatives, and presenting a common operating picture that ensures that decision-making is more informed.

e. Supporting Technologies. This component promotes national standards and interoperability for supporting technologies to successfully implement NIMS, as well as standard technologies for specific professional disciplines or incident types. It provides an architecture for science and technology support to domestic incident management.

f. Ongoing Management and Maintenance. This component establishes an activity that will provide strategic direction for and oversight of NIMS, supporting both routine maintenance and the continuous refinement of the system over the long term.

INCIDENT COMMAND SYSTEM

The Incident Command System (ICS) is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in domestic incident management. It is used to organize field-level operations for a broad spectrum of emergencies, from small to complex incidents, both natural and manmade. ICS is used by all levels of government—local, State, tribal, and Federal. It is usually organized to manage five major functional areas: command, operations, planning, logistics, and finance/administration.

1. Concepts and Principles

a. Incidents are managed locally. The initial response to most domestic incidents is handled by local first responders, and many responses will need to go no further. In those instances in which additional resources are required or are provided from within a jurisdiction across disciplines, or from outside of a jurisdiction, the ICS provides a mechanism for coordinated domestic incident management.

b. NIMS requires that field command and management functions be performed in accordance with a standard set of ICS organizations, doctrine, and procedures. Incident commanders have the flexibility to modify procedures or organization as necessary to accomplish the mission.

c. ICS is modular and scalable. ICS is designed to have the following operating characteristics:

- It is suitable for operations within a single jurisdiction or single agency, a single jurisdiction with multi-agency involvement, or multiple jurisdictions with multi-agency involvement.
- It is applicable for users throughout the country.

- It is readily adaptable to new technology.
- Its organizational structure adapts to any emergency or incident to which domestic incident management agencies would be expected to respond.
- Its staff expands or contracts in a logical manner based on the size and complexity of the incident.

d. The ICS has interactive management components that work together to provide effective domestic incident management.

e. The ICS establishes common terminology that allows disparate organizations to work together effectively.

f. The ICS incorporates measurable objectives. Measurable objectives ensure fulfillment of incident goals. Objective-setting begins at the top and filters through the entire organization.

2. Management Characteristics.

ICS is based on effective management characteristics. Each contributes to the strength and efficiency of the system.

a. Common Terminology. ICS establishes common terminology that allows diverse operational, management, and support entities to work together across a wide variety of incident management functions.

(1) Organizational Functions. Major functions and functional units of domestic incident management are named and defined. Terminology for the organizational elements is standard and consistent.

(2) Resources. Major resources, including all personnel, facilities, and major items of equipment, supplies, and facilities available at an incident, are given common names to avoid confusion. The process for accomplishing this is specified in Chapter IV.

b. Modular Organization. The incident command organization structure develops in a modular fashion based on the size and complexity of an incident. When needed, separate sections can be established, each of which may be divided into functional units. Responsibility for all functions is placed with the incident commander. As incident complexity increases, the organization expands from the top down as functional responsibilities are delegated. The

number of management positions reflects the need to adequately address the requirements of the incident.

c. **Management by Objective.** As a "top-down" procedure for obtaining desired results, management by objective starts with top management at each level of government—an agency head, a unit administrator, a district manager, or other appropriate public official—and filters down to the incident commander and on through the entire ICS organization. Management by objective includes
   - establishing strategic objectives;
   - promulgating assignments, plans, procedures, and methods;
   - establishing and directing specific, measurable objectives for various functions, in support of the strategic objectives; and
   - documenting results to describe how well the objectives are achieved.

d. **Reliance on an Incident Action Plan.** Incident Action Plans (IAP) provide a coherent means to establish and achieve the overall incident objectives.

e. **Manageable Span of Control.** Safety factors and sound management planning will influence span-of-control considerations. Within ICS, the span-of-control of any individual with incident management responsibility should range from three to seven. The type of incident, nature of the task, hazards and safety factors, and distances between resources all influence span-of-control considerations.

f. **Designated Incident Locations and Facilities.** There may be various types of locations/facilities established near the incident area for various purposes, such as decontamination, donated goods, etc., The identification and location of facilities are based upon the requirements of the incident at the direction of the Incident Commander.

g. **Comprehensive Resource Management**. Resource management includes processes for categorizing, allocating, acquiring, tracking, and deploying resources. Resources are defined as personnel, equipment, supplies, and facilities available or potentially available for assignment or allocation.

h. **Integrated Communications**. All entities involved in domestic incident management will use a common communications plan. This plan links the tactical and support units of the various agencies and is necessary to maintain communications discipline. Preparedness planning must address equipment,

systems, and protocols necessary to achieve integrated voice and data communications.

i. **Establishment and Transfer of Command.** The command function must be clearly established from the beginning of incident operations. The agency with primary jurisdiction at the scene designates the most qualified individual at the scene to establish command. When command is transferred, the process must include a briefing that captures all essential information for continuing effective command.

j. **Chain of Command and Unity of Command.** *Chain of command* refers to the orderly line of authority within the ranks of the organization. *Unity of command* means that every individual has a designated supervisor to whom they report at the scene of the incident. These principles clarify reporting relationships and eliminate the confusion caused by multiple, conflicting directives. Incident managers must be able to control the position and function of all personnel under their supervision.

k. **Reliance on Unified of Command.** In incidents involving multiple jurisdictions a unified command allows agencies with different legal, geographic, and functional responsibilities to work together effectively.

l. **Accountability.** Effective accountability during domestic incident management is essential. To that end, the following processes must be established:

- Check-In. All responders, regardless of agency affiliation, must report in accordance with the procedures established by the incident commander to receive a mission assignment.
- Incident Action Plan. Tactical operations must be directed and coordinated as outlined in the IAP.
- Unity of Command. Each individual involved in domestic incident management will be assigned to only one supervisor.
- Span of Control. Supervisors must be able to adequately supervise and control their subordinates. Division or group supervisors must be able to communicate with and control all resources under their supervision.
- Unit or Branch Assignment Lists. Resources with active assignments in the Operations Section must be identified.

- Resource Tracking. Resources with active assignments must be identified on unit or branch assignment lists. Each supervisor will record and report resource status changes as they occur.

m. Deployment. Personnel and equipment should only respond when requested or when dispatched by an appropriate authority.

n. Information and Intelligence Management. There must be an established process for gathering and managing incident-related information.

3. ICS Organization and Operations.

a. Command and General Staff Overview.

The ICS organization has five major functions, as described in Figure 1. These are command, operations, planning, logistics, and finance and administration (with a potential sixth functional area to cover the Intelligence function as described in paragraph 3.n. above).

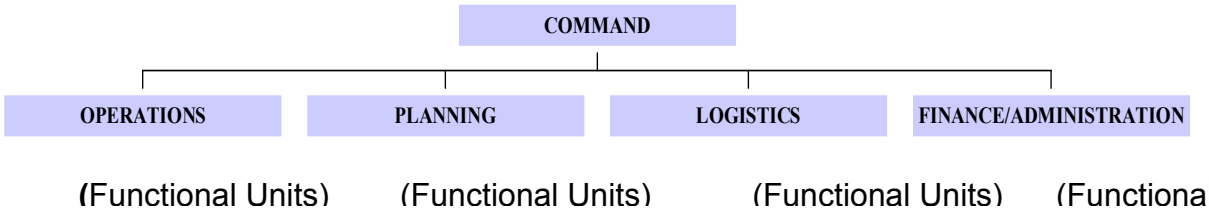
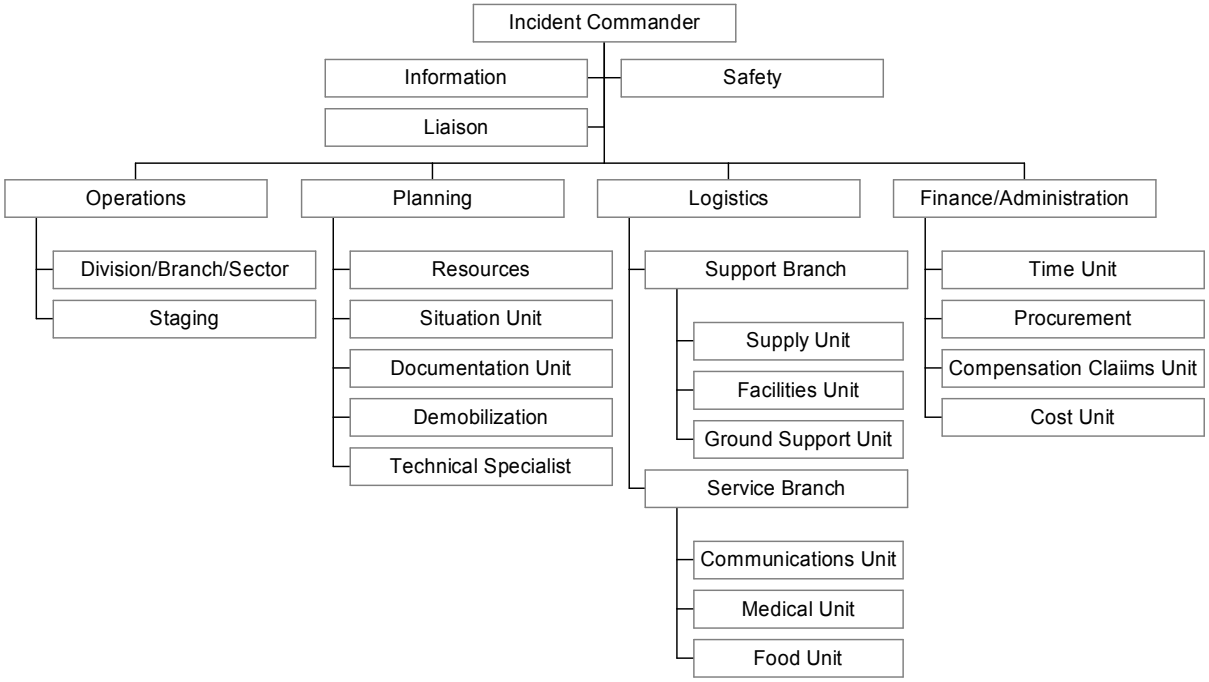


Figure 1 - Incident Command System: Command Staff and General Staff

Fully Developed Incident Command Structure



(1) Command staff is composed of the Incident Commander and his immediate staff. Positions are established to assume responsibility for key activities, which are not a part of the line organization. These positions may include the Information Officer, Safety Officer, and Liaison Officers.

(2) General staff is composed of the group of domestic incident management personnel that represent the major functional or "line" elements of any command to include the operations section chief, planning section chief, logistics section chief, and finance and administration section chief.

Information on the specific functions and makeup of the units within each section is located in the Appendices.

b. The Command Staff.

The command element is responsible for overall management of the incident. This includes certain staff functions required to support the command function.

(1) The Command Function

The command function may be conducted in two general ways:

(a) Single Command Incident Commander/Deputy. When an incident occurs within a single jurisdiction and there is no jurisdictional overlap, a single Incident Commander (IC) should be designated by the jurisdictional agency to have overall management responsibility for the incident.

The Incident Commander will prepare Incident Objectives upon which subsequent incident action planning will be based. The Incident Commander will approve the IAP and approve all requests for ordering and releasing of incident resources.

(b) Unified Command. UC is an important element in multi-jurisdictional domestic incident management. It provides guidelines for agencies with different legal, geographic, and functional responsibilities to work together effectively. UC overcomes much of the inefficiency and duplication of effort that can occur when agencies with functional and geographic jurisdictions, or agencies at different levels of government, work together without a common system. All agencies with jurisdictional responsibility at a multi-jurisdictional incident participate in the UC and contribute to the process of determining overall incident strategies; selecting objectives; ensuring that joint planning for tactical activities is accomplished in accordance with approved incident objectives; ensuring the integration of tactical operations; and making maximum use of all assigned resources. The proper selection of participants to work within a UC structure depends upon the location of the incident (which geographical administrative jurisdictions are involved) and the type of incident (which functional agencies of the involved jurisdiction(s) are required).

(i) Incident commanders represent different legal authorities and use a collaborative process to establish incident priorities that accommodate those authorities. Agencies heavily involved in the

incident, which lack jurisdictional responsibility, are represented in the command structure through the liaison officers. Jurisdictional responsibilities of multiple incident commanders are consolidated into a single planning process, including

- responsibilities for incident mitigation;
- incident objectives;
- resource availability and capabilities;
- limitations; and
- areas of agreement and disagreement between incident commanders.

(ii) Each incident is managed under a single, collaborative approach, including

- one organizational structure;
- one incident command post;
- one planning process; and
- one resource management process.

(iii) Under UC, a single individual, the Operations Section Chief (OSC) will direct the tactical implementation of the IAP. The OSC will normally come from the agency with the greatest jurisdictional involvement. UC will agree on the designation of the OSC. Unified command works best when incident commanders are collocated at an incident command post and observe the following practices:

- Select one Operations Section Chief (OSC) for each operational period.
- Keep each other informed of specific requirements.
- Establish consolidated incident objectives, priorities, and strategies.
- Coordinate to establish a single system for ordering resources.
- Develop a consolidated IAP, written or verbal; evaluated and updated at regular intervals.
- Establish procedures for joint decision-making.

(iv) The primary differences between the single command structure and the unified command structure are:

- In a single command structure, the incident commander is solely responsible (within the confines of his or her authority) to establish objectives and overall management strategy associated with the incident. The incident commander is directly responsible for

ensuring that all functional area actions are directed toward accomplishment of the strategy.

- In a unified command structure, the individuals designated by their jurisdictions (or by departments within a single jurisdiction) must jointly determine objectives, strategies, and priorities.

(2) Staff Officer Functions

Members of the command staff assume responsibility for key activities that are not a part of the line organization. Three specific staff positions have been identified:

(a) Information Officer: The information officer develops accurate and complete information on the incident's cause, size, and current situation; on the resources committed thus far; and on other matters of general interest. The information officer is generally the point of contact for the media and other governmental agencies that desire information directly from the incident. Whether the command structure is single or unified, only one information officer should be designated. Assistants may be assigned from other agencies or departments involved. The ICs must approve all incident information that the information officer releases.

(b) Safety Officer: The safety officer assesses hazardous and unsafe situations and develops measures for ensuring personnel safety. The safety officer should have emergency authority to stop and/or prevent unsafe acts. In a UC structure, a single safety officer should be designated, despite the multiple jurisdictions involved. Assistants may be required and may be assigned from other agencies or departments making up the UC.

(c) Liaison Officer: The liaison officer is the point of contact for representatives of other agencies. In either a single or unified command structure, representatives from assisting or cooperating agencies would coordinate through the liaison officer. Agency representatives assigned to an incident should have the authority to speak for their own agencies

on all matters. Assistants may be assigned from other agencies or departments involved with the incident.

In the context of large or complex incidents, command staff members may need one or more assistants to manage their workloads. Each command staff member is responsible for organizing his or her assistants for maximum efficiency. Additional positions might be required, depending upon the nature and location of the incident, or requirements established by the IC (for example, an intelligence officer, if sensitive information needs to be managed).

c. The General Staff.

The general staff is responsible for the functional or "line" elements of any command; it consists of the following components:

Operations Section. Tactical operations at the incident include all activities directed toward reduction of the immediate hazard, establishing situation control, and restoration of normal operations.

Figure 2 shows the primary organizational structure within the Operations Section. However, several different ways to organize domestic incident management operations are acceptable. In some cases, the selected method will be determined based upon jurisdictional boundaries. In other cases, a strictly functional approach will be used. In still others, a mix of functional and geographical considerations may be appropriate. The ICS offers flexibility in determining the right approach based on specific circumstances of the incident at hand.

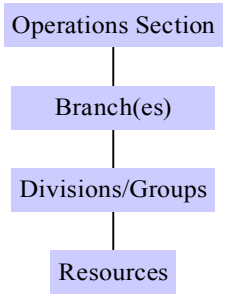


Figure 2 - Major Organizational Elements of Operations Section

(a) **Operations Chief and Deputies**. The Operations Section Chief (OSC) is responsible for the direct management of all incident tactical activities. The OSC will establish tactical objectives for each operational period, with all section chiefs and unit leaders establishing their own supporting objectives. The section chief may have one or more deputies assigned, with deputies from other agencies encouraged in multijurisdictional incidents. A section chief should be designated for each operational period and should have direct involvement in the preparation of the IAP for the period of responsibility.

(b) **Branches.** Branches may be established to serve several purposes. In general, branches are established when the number of divisions or groups exceeds the recommended span of control of 3:1 to 7:1 for the OSC.

(c) **Divisions and Groups.** Divisions and Groups are established when the number of resources exceeds the span of control of the Operations Section Chief. Divisions are established to divide an incident into physical or geographical areas of operation. Groups are established to divide the incident into functional areas of operation. For certain types of incidents, for example, the IC may establish intelligence functions as a functional group in the operations section.

Planning Section. The Planning Section collects, evaluates and disseminates incident situation information (including unclassified intelligence information), prepares status reports, displays situation information, maintains status of resources assigned to the incident, and develops the IAP.

As shown in Figure 3, the Planning Section has four primary units and may have a number of technical specialists to assist in evaluating the situation and forecasting requirements for additional personnel and equipment.

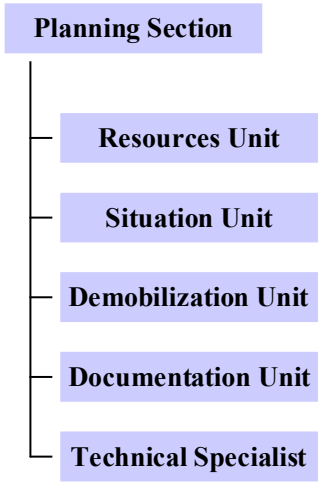


Figure 3 - Planning Section Organization

The Planning section is usually responsible for gathering and disseminating information critical to the incident, unless the incident commander places the function elsewhere. Traditionally, information and intelligence functions are located in the Planning Section.

The Planning Section is also responsible for developing the IAP. The IAP should include the overall incident objectives strategies established by the incident commander or the UC. In the case of UC, the incident objectives should adequately address the mission and policy needs of each jurisdictional agency. It should also address tactical objectives and support

activities required for one operational period, generally 12 to 24 hours. The IAP is especially important when

(a) multiple agency resources are being used;

(b) several jurisdictions are involved; or

(c) changes in shifts of personnel and/or equipment are required.

The plan may be oral or written. When written, the plan will typically contain a number of components as shown in Figure 4.[1]

Common Components:	Normally Prepared By:
1. Incident Briefing	Incident Commander
2. Incident Objectives	Planning Section Chief
3. Organization List/Chart	Resources Unit
4. Assignment List	Resources Unit
5. Communications Plan	Communications Unit
6. Logistics Plan	Resources Unit
7. Medical Plan	Medical Unit
8. Incident Map	Situation Unit
9. Safety Plan	Safety Officer
Other Potential Components	
1. Air Operations Summary	Air Operations
2. Traffic Plan	Ground Support Unit
3. Decontamination Plan	Technical Specialist
4. Waste Management or Disposal Plan	Technical Specialist
5. Demobilization Plan	Demobilization Unit

Figure 4 - Sample IAP Outline

Logistics Section. The Logistics Section (Figure 5) provides all support needs to the incident, including ordering resources from off-incident locations. It also provides facilities, transportation, supplies, equipment maintenance and fuel, food services, communications and information technology support, and medical services.

[1] For full descriptions of units in each ICS section, see the Tabs in Appendix A.

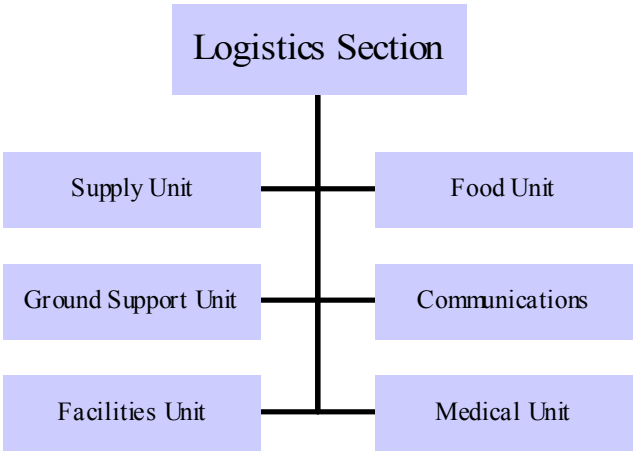


Figure 5 - Logistics Section Organization

Finance and Administration Section. A Finance and Administration Section is established when the agency(s) involved in an incident require(s) finance and other administrative services. Not all agencies will require a separate Finance and Administration Section. In cases that require only one specific function (e.g., cost analysis), the service can be provided by a technical specialist in the planning section. The basic organizational structure for a Finance and Administration Section is shown in Figure 6. When such a section is established, the depicted units may be created as required. The Appendices provide information relative to the function and responsibilities of each unit.

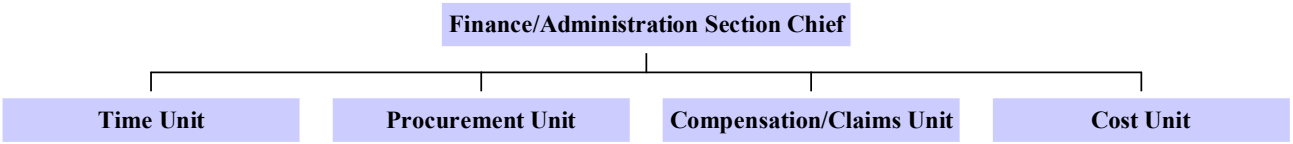


Figure 6 - Finance and Administration Section Organization

Information and intelligence function. The sharing of information and intelligence is an important component of ICS. In this context, intelligence includes not only national security or other types of *classified* information but also

other operational information, such as risk assessments, weather information, geospatial data, structural designs, and utilities and public works data that may come from a variety of sources. Traditionally, information and intelligence functions are located in the Planning Section. However, in exceptional situations, the Incident Commander may need to assign the information and intelligence functions to other parts of the ICS organization. In any case, intelligence must be shared with personnel, designated by the Incident Commander who have "need-to-know" to ensure that it supports decision-making.

The intelligence function in an incident may be organized in one of the following ways:

- Within the Command staff. This option may be most appropriate in incidents with little need for tactical intelligence, and where the intelligence is provided by supporting Agency Representatives, through real-time reach-back capabilities.
- As a branch within the Planning (and Intelligence) Section. This option may be most appropriate in incidents with some need for tactical intelligence, and where a law enforcement entity is not a member of the UC.
- As a branch within the Operations Section. This option may be most appropriate in incidents with a high need for tactical intelligence, and where law enforcement is a member of the UC.
- As separate section, which may be most appropriate where an incident heavily driven by intelligence factors.

4. Area Command

a. Description

An area command is activated only if necessary, depending upon the incident's complexity and span of control considerations. An agency administrator or other public official with jurisdictional responsibility for the incident usually makes the decision to establish an area command. An area command is established either to oversee the management of multiple incidents that are each being handled by an ICS organization or to oversee the management of a very large incident that has

multiple incident management teams. Area command is used when there are a number of incidents in the same area and of the same type, such as two or more hazardous materials (HAZMAT) or oil spills, and fires. These are the kinds of incidents that might compete for the same resources. When incidents do not have similar resource demands, they are usually handled as separate incidents and are coordinated through an Emergency Operations Center (EOC). If the incidents under the authority of the Area Command are multi-jurisdictional, then a Unified Area Command should be established. This allows each jurisdiction to have representation in the Area Command. Area command should not be confused with an EOC. An area command has direct command authority over the incident commander(s) while an EOC coordinates support functions and provides resources support.

b. Responsibilities. For the incidents under its authority, an area command has the responsibility to:

- set overall incident-related priorities;
- allocate critical resources based on priorities;
- ensure that incidents are properly managed;
- ensure that domestic incident management objectives are met and do not conflict with each other or with agency policy;
- identify critical resource needs and report them to EOCs; and
- ensure that short-term emergency recovery is coordinated to assist in transition to full recovery operations.

See the Appendices for additional information and guidance on area commands.

B. MULTIAGENCY COORDINATION SYSTEMS.

1. Definition.

Multiagency coordination systems are a combination of facilities, equipment, personnel, procedures, and communications integrated into a common system with responsibility for coordinating and supporting domestic incident management activities. The primary functions of multiagency coordination systems are to establish domestic incident management policies and priorities, to provide logistics

and track resources in support of domestic incident management activities, to allocate limited resources based on domestic incident management priorities, to coordinate incident related information, and to coordinate inter-agency and inter-governmental decisions on domestic incident management policies, priorities, and strategies. Tactical and operational responsibility to domestic incident management activities remains with incident commanders.

2. System Elements.

Multi-agency coordination systems may contain three principal elements: emergency operations centers, multi-agency coordinating entities (in the context of certain multi-jurisdictional or complex incident management scenarios), and joint information systems.

a. Emergency Operations Center. An EOC is a physical location for coordination of assistance in support of domestic incident management activities. These centers may alternatively be called command centers, situation rooms, crisis management centers, or other similar terms. Regardless of the term used, EOCs represent the physical location where the coordination of information and resources to support domestic incident management activities normally takes place. Emergency operations centers may be organized by major functional disciplines (fire, law enforcement, medical services, and so on), by jurisdiction (city, county, region, and so on), or some combination thereof.

Emergency operations centers may be permanent organizations and facilities or may be established to meet temporary, short-term needs. The physical size, staffing, and equipping of an EOC will depend on the size and capability of the jurisdiction and the expected workload required of the EOC. EOCs may be organized and staffed in a variety of ways. Regardless of the specific organization, EOCs must include the following core functions: command and management, communications, resource dispatch and tracking, planning, and information collection, analysis, and dissemination. EOCs may also support multiagency coordination and joint information activities as discussed below.

EOCs at all levels of government must be capable of communicating appropriately with other EOCs. The efficient functioning of EOCs depends on the existence of mutual aid agreements among participating agencies. Such agreements are discussed in Chapter III.

b. Multi-agency Coordination Entities. In the case of incidents that cross disciplinary or jurisdictional boundaries or those that involve complex incident management scenarios, a multi-agency coordination entity may be used to facilitate domestic incident management. The situation at hand and the needs of the jurisdictions involved will dictate how these multi-agency coordination entities conduct their business, as well as how they are structured. Multi-agency coordination entities typically consist of principals (or their designees) from organizations and agencies with direct incident management responsibility or with significant incident management support or resource responsibilities. These entities are often referred to as crisis action teams, policy committees, incident management groups, executive teams, or other similar terms.[2] In many cases, emergency operations centers serve a dual function as a multi-agency coordination entity; in others, the preparedness organizations discussed in Chapter III may fulfill this role. Regardless of the term or organizational structure used, these entities typically provide strategic direction during domestic incidents. If constituted separately, multi-agency coordination entities, preparedness organizations, and emergency operations centers must coordinate and communicate with one another to provide uniform and consistent guidance to incident management personnel.

Regardless of form or structure, the principal functions and responsibilities of the multi-agency coordination entity typically include the following:

- ensure that each agency involved in domestic incident management activities is providing appropriate situational awareness and resource status information;

[2] For example, the wildland fire community has such an entity called the Multi-Agency Coordination Group (MAC Group).

- establish domestic incident management priorities;
- acquire resources required by incident management personnel;
- anticipate and identify future resource requirements;
- resolve policy issues arising from the incident; and
- provide strategic direction as required.

Following incidents, multi-agency coordination entities are also typically responsible for ensuring that improvements in plans, procedures, communications, staffing, and other capabilities necessary for enhanced incident management are acted upon. These improvements should also be coordinated with appropriate preparedness organizations (See Chapter III), if these organizations are constituted separately.

C. PUBLIC INFORMATION SYSTEMS.

Systems and procedures for communicating timely and accurate information to the public are critical during crisis or emergency situations. This section describes the principles, system components, and procedures needed to support effective emergency public information operations.

1. Public Information Principles.

a. Public Information Officer supports the Incident Command. Under the ICS, a Public Information Officer (PIO) is a key staff member supporting the command structure. The PIO represents and advises the Incident Command on all public information matters relating to the incident management. PIO handles media and public inquiries, emergency public information; rumor monitoring and response, media monitoring, and other functions required to disseminate information related to the incident. PIO is also responsible for coordinating public information at or near the incident site and serving as the on-scene link to the Joint Information System (JIS). In a large-scale operation, the on-scene PIO serves as a field PIO with links to the appropriate Joint Information Center (JIC) at the local, State, regional or Federal emergency operations center. The JIS provides the mechanism for integrating public information activities among JICs, across jurisdictions, and with the private sector.

b. Public information functions must be coordinated and integrated across jurisdictions; among local, State, Tribal, and Federal partners; and with the private sector. During emergencies, the public may receive information from a variety of sources. The JIC provides a location for organizations participating in the management of an incident to work together to ensure that timely, accurate, easy-to-understand, and consistent information is disseminated to the public. The JIC comprises representatives from each organization involved in management of an incident. In large or complex incidents, JICs may be established at various levels of government. All JICs must communicate and coordinate with each other on a continuous basis.

c. Organizations participating in an incident management retain independence. MAC Groups are responsible for establishing and overseeing JICs to include processes for coordinating and clearing public communications. As with UC, the departments, agencies, organizations, or jurisdictions that contribute to joint public information do not lose their individual identities or responsibility for their own programs or policies. Rather, each entity contributes the overall unified message.